Taiwan and the RMA

James Mulvenon
The RAND Corporation

Introduction

Not all Revolutions in Military Affairs (RMA) are created equal. One interesting dimension is the depth of information technology penetration in a given country. For countries with high levels of information technology and a well-educated, information-savvy population, RMAs have the potential to be "deep," forming layers of links with the private sector and feeding off the technological dynamism of industry. For developing countries, however, RMAs can be imported at high cost, but the potential impact is likely to be more "shallow." Using this distinction, the Gulf War might therefore be seen as a conflict between a deep RMA (USA) and a shallow RMA (Iraq). At first glance, the emerging conflict between China and Taiwan appears to also follow this pattern, with Taiwan enjoying a potentially deep RMA and China importing the more shallow variety. While an enormous amount of research has been conducted on the Chinese side of the equation, little if any attention has been given to RMA trends in Taiwan. This paper seeks to fill this gap, examining both the technological base and military policies of Taiwan to forge an assessment of its military modernization. *The preliminary finding is that Taiwan is blessed with many technological and economic precursors to a deep RMA, but that largely political and bureaucratic constraints have thus far impeded a full exploitation of this potential capability.*

This paper is divided into two large sections. The first addresses the social, economic, and technological base in Taiwan to support an RMA. The second outlines the current state of the RMA in Taiwan, beginning with an assessment of the Chinese threat that is driving the process. The section then procedes with an analysis of overall RMA policy, followed by an examination of Taiwanese programs in a variety of RMA-related areas, including electronic warfare, C4ISR, and computer network warfare.

Taiwan and the Information Revolution: Society, Economy, and Technology

By almost any metric, Taiwan is one of the most "wired" countries in the world. In terms of demographics, Taiwanese society is a cutting-edge, "early adopter" with a deep penetration of information technologies, and conscripts from this population bring a high level of comfort with technology to their military service. Taiwan's overall teledensity (telephone subscribers per 100 populations) is 48%, one of the top twenty in the world. While this distribution rate is lower than most countries in Europe and the U.S., the only Asian countries with higher rates are the thoroughly wired Hong Kong and Japan. Taiwan's Directorate General of Telecommunications (DGT) announced in January 1999 that the number of cell phone subscribers in Taiwan increased to more than 10 million, which equates to approximately 45 percent of the island's population of 22 million. In comparison with other wired countries in Asia, Singapore's cellular teledensity is 44.63 percent, Japan's is 42.98 percent and Hong Kong's reached 59.43 percent by the end of 1999. Nearly 48.9% of the public switched telephone network subscribers also own cellular phones.[1] As for the Internet, Taiwan's active Internet users in July 1999 numbered 4.13 million, representing an increase of one million from December 1998. In comparative terms, Taiwan ranks eighth in the world in terms of the number of Internet users, ninth in terms of Internet penetration at 18.8 percent, and seventh in the world (third with regard to the Asia-Pacific region, just after Japan and Australia) in terms of Internet hosts, which totaled nearly 677,000, up 30 percent from January 1999.

Not surprisingly, Taiwan's information-savvy population enjoys one of the world's most advanced information infrastructures, and many features of this infrastructure can be considered dual-use assets for a military pursuing an RMA. Taiwan's civilian telecommunications infrastructure consists of a nationwide network of fixed telephone lines (coaxial and fiber optic), microwave, wireless (satellite, cellular, paging), and TV and radio broadcast. Taiwan is rapidly developing its telecommunications infrastructure with the goal of becoming an Asia-Pacific telecommunications hub, and the Taiwan military is likely to benefit from any improvements to the commercial architecture.[2]

At an economic and technological level, the Taiwanese industrial and service sectors are world leaders in information technologies, and provide an outstanding base for the research, development, and production of most RMA-related systems. To reach this status, Taiwan followed the path of Japan and Korea, moving from assembly of foreign components to cutting-edge research and state-of-the-art production. The island has been the world's third-largest computer hardware supplier since 1995, trailing only the United States and Japan, and the information and electronics industries now account for almost 30 percent of the island's manufacturing output. This highly advanced technology base and research infrastructure offers enormous potential spin-off benefits for Taiwan's defense R&D apparatus, particularly in electronic- and information-intensive RMA technologies.

Yet the RMA environment in Taiwan is not entirely positive. The modernity of Taiwan's telecommunications infrastructure and the ubiquity of information technologies in Taiwan society represent some of Taiwan's greatest potential vulnerabilities. Like all nations that are heavily reliant on a computer-driven way of life, the island is potentially vulnerable to critical infrastructure attacks, ranging from computer network attack to electronic attack to electromagnetic pulse weapons to fifth column sabotage.[3] Moreover, Taiwan's advanced information industry is a necessary but not sufficient condition for a deep RMA. The island's diplomatic and military isolation, coupled with an arms procurement process driven as much by political as warfighting considerations, distorts its modernization process, preventing full actualization of the island's potential RMA capability.

The RMA and the Taiwanese Military
Overall Assessment

The Taiwan defense establishment has publicly expressed its commitment to the implementation of an RMA. The primary driver for the island's RMA is China's military modernization and

[1] Data from the International Telecommunications Union, 2001.

[2] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

[3] 2000 White Paper.

growing coercive threat. At the same time, Taiwan's RMA process intersects with the ongoing evolution of its military strategy from a defensive to offensive orientation, including elements of electronic warfare, C4I and information warfare. Currently, the ROC military is an early stage of the RMA, reforming its organizational structure and upgrading its core C4I structure to facilitate future implementation of a full-spectrum RMA. These reforms are proceeding gradually, aided in part by augmented military-to-military exchanges with the U.S., resulting in a military force that combines pre-RMA and nascent RMA components.

The Milieu: The China Threat

The RMA in Taiwan, like most military revolutions, is driven largely by outside factors, in this case China's military modernization and increasingly bellicose attitude towards political trends on the island. Democratizing trends begun in Taiwan in the mid- to late-1980s have unleashed an unprecedented pluralism in Taiwan, including discussion of formal independence from the mainland, which is anathema to Beijing. In response to these trends, China in the early 1990s initiated a program of military modernization designed to increase the credibility of its ability to coerce the island to accept reunification. The PRC began aggressively importing advanced weapons systems from Russia to fill certain Taiwan-related niche capabilities and deploying them in the provinces opposite the island. Taiwan's political evolution and Chinese military developments intersected in 1995 and 1996, when China responded to the visit of Taiwan's president to the United States by engaging in provocative saber-rattling with large-scale exercises and ballistic missile tests.

As a result of the 1995-1996 tensions, China's weapons programs now place an increased emphasis on acquiring capabilities designed to strengthen the credibility of Beijing's military options against two identified *schwerpunkt* in a Taiwan scenario: the will of the Taiwanese people, which China hopes to shape with stand-off terror weapons like ASCMs, long-range LACMs, and SRBMs, and U.S. military intervention in a China-Taiwan conflict, which China hopes to shape with long-range, anti-ship cruise missiles and submarines. In addition to these conventional systems, the Chinese military appears to be actively exploring a variety of RMA-related technologies, including satellite and reconnaissance technology; electronic, computer, microwave, laser and other radio transmission technology; and electromagnetic weapons. Current modernization programs seek to realize short-term improvements in anti- surface warfare (ASuW) and precision strike, as well as and longer term advances in missile defense, counter-space, and information warfare (IW) writ large. Beijing also is working to address problems associated with integrating advanced weapons systems into their inventory, weaknesses in C4I, deficiencies in training, and new challenges in logistics, so as to improve the PLA's overall warfighting capability.[4]

For some in the PLA, the synergy of these technologies offer the potential of asymmetrically breaching Taiwan's national security by sabotaging, manipulating, and disrupting Taiwan's national decision-making mechanism and central command system. The June 2000 Pentagon report on Chinese military power outlines this strategy:

[4] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

> By launching swift strikes with elite units and focusing on the enemy's potential vulnerabilities, China can deal "symmetrical" blows at the enemy with "asymmetrical" methods. "Winning the battle piecemeal" means destroying selective reconnaissance, electronic and support systems in order to disrupt and reduce the effectiveness of the enemy's coordinated air operations. Combining information warfare--such as computer hacking--with irregular special and guerilla operations, would allow China to mount destructive attacks within the enemy's own operations systems, while avoiding a major head-on confrontation.[5]

The threat from these developments has also clearly been recognized in Taiwan, as evidenced by former Defense Minister Tang Fei's remarks in March 1999 that the Chinese were in the midst of full-force development of "electronic warfare" military technologies, including smart bombs, computer viruses, and electromagnetic pulse weapons, with the aim of "punching" Taiwan's "pressure points".[6]

Electronic Warfare. Two similar assessments of Chinese electronic warfare capability are offered by the Taiwan military and the U.S. Department of Defense. In its 1999 report entitled "The Security Situation in the Taiwan Strait," the Pentagon summarized the state of Chinese EW activities as follows:

> The thrust of China's electronic warfare (EW) efforts continues to focus on technology development and design capabilities improvement, accomplished mainly through cooperation with Western companies, through reverse engineering efforts, and through the procurement of foreign systems. The inventory of Chinese EW equipment includes a combination of 1950s-1980s technologies, with only a few select military units receiving the most modern components. China is procuring state-of-the-art technology to improve its intercept, direction finding, and jamming capabilities. In addition to providing extended imagery reconnaissance and surveillance and ELINT collection, Beijing's unmanned aerial vehicle programs probably will yield platforms for improved radio and radar jammers. Additionally, existing earth stations can be modified to interfere with satellite communications. Finally, the PLA is developing an electronic countermeasures (ECM) doctrine and has performed structured training in an ECM environment.[7]

The perceived operational purpose of these developments was outlined in a June 2000 edition of the "Annual Report on the Military Power of the People's Republic of China":

> PLA EW operations against air defense radars, disruption of command and control networks, and/or large scale conventional SRBM and LACM strikes

[5] Office of the Secretary of Defense, "Annual Report On The Military Power Of The People's Republic Of China," Report to Congress Pursuant to the FY2000 National Defense Authorization Act, 22 June 2000.

[6] Zheng Jian, "The Unseen Front: 'Pressure Point War' and the 'Network Security Plan'," *Bingqi Zhishi*, 4 July 1999, pp.9-11.

[7] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

> against airfields and SAM sites could reduce the effectiveness of Taiwan's air defenses.[8]

These assessments are largely seconded by Taiwanese military officials. In May 1999, General Tang Fei and several other officials were invited by a Legislative Yuan committee to report on the state of electronic warfare across the Taiwan Strait.[9] General Tang told the legislators that mainland China was expected to establish an electronic warfare supremacy by 2010. Facing the threat from mainland China, Tang stressed that Taiwan should strive to renovate its defense systems and consolidate related sectors, so as to ensure its security.

Information Warfare. The June 2000 Annual Report on Chinese Military Power" provided an overall assessment of Chinese IO developments, arguing:

> China increasingly is viewing Information Operations/Information Warfare (IO/IW) as a strategic weapon to use outside of traditional operational boundaries. Yet China's information warfare (IW) program is in the early stages of research. It currently focuses on understanding IW as a military threat, developing effective countermeasures, and studying offensive employment of IW against foreign economic, logistics, and C4I systems. While the PLA's theoretical research on IW is fairly mature, the Chinese military has not yet developed a coordinated and integrated IW doctrine to match its maturing theory.[10]

This comprehensive program on information operations has focused particularly on computer network operations, including a short-term emphasis on computer network defense:

> Driven by the perception that China's information systems are vulnerable, the highest priority has been assigned to defensive IW programs and indigenous information technology development. Some technologies could provide enhanced defensive or offensive capabilities against Taiwan military and civilian information infrastructure systems. Computer anti-virus solutions, network security, and advanced data communications technologies are a few examples. Chinese open source articles claim that the PLA has incorporated IW-related scenarios into several recent operational exercises. Efforts have focused on increasing the PLA's proficiency in defensive measures, especially against computer viruses.[11]

Over the longer-term, however, China is clear interested in offensive options for computer network warfare:

> In the particular realm of Computer Network Attack, China appears interested in researching methods to insert computer viruses into foreign networks as part of its

[8] Office of the Secretary of Defense, "Annual Report On The Military Power Of The People's Republic Of China," Report to Congress Pursuant to the FY2000 National Defense Authorization Act, 22 June 2000.

[9] "Tang Fei: PRC May Have Electronic War Supremacy by 2010," *Taiwan Central News Agency*, 05 May 1999.

[10] Office of the Secretary of Defense, "Annual Report On The Military Power Of The People's Republic Of China," Report to Congress Pursuant to the FY2000 National Defense Authorization Act, 22 June 2000.

[11] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

> overall Information Operations (IO) strategy. Beijing reportedly has adequate hardware and software tools and possesses a strong and growing understanding of the technologies involved. China's strategic IO use of advanced information technologies in the short- to mid-term likely will lack depth and sophistication; however, as it develops more expertise in defending its own networks against enemy attack, it is likely to step up attempts to penetrate adversarial information systems.[12]

Yet the Chinese have many challenges to overcome and Beijing's ability to paralyze Taiwan's command and control currently appears limited at best, though the growing institutionalization of its computer network operations programs strongly suggests an evolving maturity in the PRC's computer network attack capability.

From the Taiwan perspective, Chinese information attack is treated as a serious threat by officials at the highest levels of the government and military. In May 1998, then Defense Minister Tang Fei stated that by the year 2010, Taiwan could face the danger of an attack on its information infrastructure from the mainland. In early 1999, Chief of the General Staff Tang Yao-ming warned that the mainland might launch an "information war to paralyze military command as well as energy, transportation, and banking systems before an invasion of Taiwan.[13] A November 1999 administrative report, however, revised Tang Fei's earlier temporal assessment, predicting that such a Chinese information attack could come as early as 2005.[14] The continuing scale and seriousness of the Chinese effort was highlighted in March 2000 by the Taiwan military officer directly charged with countering the threat, General Lin Chi-cheng of the Communications, Electronics, and Information Bureau (CEIB), who argued that the PRC was mobilizing the development of information warfare at the national level and therefore exceeding corresponding Taiwan efforts at the levels of science and technology, budget, manpower, policy guidance, and troop implementation.[15] Additional, concrete evidence of the PRC's efforts was offered by General Lin, who asserted that the mainland has been attempting to paralyze parts of Taiwan's national defense, transportation, and financial infrastructure by launching tens of thousands of information warfare attacks during the March 2000 presidential election. These attacks were similar in scope and scale to the mainland's cyberattacks against Taiwan in August 1999, which were linked to a perceived increase in pro-independence sentiment on the island. Those earlier strikes targeted sensitive military computers, transportation and shipping facilities, and financial computer networks.[16]

The Evolution of Taiwan's Military Strategy: From Defense to Offense

In the realm of defense policy, Taiwan is pursuing a variety of objectives, keyed to the need to deter the Mainland and to reassure the Taiwan public that it is secure from attack. On the most basic level, Taipei desires to possess a credible deterrent or other adequate countermeasures against all likely PRC military threats, through the formulation of an appropriate military

[12] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

[13] "Military to Test Computer Bugs," *AFP*, 8 August 2000.

[14] "Defense minister calls for budget increase," *China Times*, 2 November 1999.

[15] Lin Chin-ching, "Comparison of PRC, ROC Information Warfare Capabilities," 1 March 2000, pp.68-73.

[16] "Army says mainland cyberattacks thwarted," *Liberty Times*, 14 March 2000.

doctrine and related operational guidelines for the ROC military as well as the maintenance of a corresponding force structure and C4I / logistics infrastructure.[17] To this end, Taiwan has embarked on an identifiably program of military modernization, including reform of military strategy, organizational structure, force structure, weapons systems, and C4I infrastructure. While the majority of this modernization is not at all revolutionary in intent or scope, elements of the RMA pervade nearly every sector.

In the early nineties, when the ROC government formally abolished its longstanding emphasis on retaking the Chinese Mainland, Taiwan's military doctrine shifted from an emphasis on unified offensive-defensive operations (*gong shou yi ti*) to a purely defensive-oriented concept (*shoushi fangyu*) which excluded provocative or preemptive military actions against the Mainland.[18] This purely defensive posture contained two strategic notions: "resolute defense" (*fangwei gushou*) and "effective deterrence" (*youxiao hezu*). The former concept was largely political and defensive, connoting the determination of the Taiwan military to defend all the areas directly under its control without giving up any territory. The latter concept was more active and forward-oriented, underlining the commitment to building and maintaining a military capability sufficient to severely punish any threatening or attacking force and to deny such a force the attainment of its objectives, thereby deterring it from initiating an assault against Taiwan.[19]

To implement this strategy, Taiwan's military forces needed to succeed in carrying out three key missions, listed in general order of priority: 1) air superiority (*zhikong*) for the ROC Air Force; 2) sea denial (*zhihai*) for the ROC Navy; and 3) anti-landing warfare (*fandenglu*) for the ROC Army.[20] Each of these missions was generally viewed by each service as constituting a relatively separate and distinct task. In other words, Taiwan's defense strategy was not focused on joint warfighting. This was reportedly due in part to the small size of the ROC military, the limited expanse of the battlespaces involved, the limited technical capabilities of Taiwan's weapons systems, and the purely defensive nature of the mission given to each service. It also reflected the severe restrictions on operational capabilities imposed by Taiwan's relatively small defense budget, which did not permit even the most basic, individual mission of each service to be fully implemented.[21] More broadly, the separate warfighting missions of each military service reflected the larger "stovepiped" nature of the ROC military structure as a whole.[22]

[17] Much of the following description of Taiwan's defense doctrine and related military policies is excerpted from Michael D. Swaine, *Taiwan's National Security, Defense Policy, and Weapons Procurement Processes*, RAND, MR-1128-OSD. Santa Monica, California, 1999, pp.51-61.

[18] Alexander Chieh-cheng Huang, "Taiwan's View of Military Balance and the Challenge It Presents," in James R. Lilley and Chuck Downs, eds., *Crisis in the Taiwan Strait*, National Defense University Press, Washington D.C., September 1997, pp.282-283.

[19] Alexander Huang, 1997, pp.284-285

[20] The first two missions reportedly enjoy the highest priority, given the importance of air and sea denial capabilities to preventing air or missile attacks, blockades, and invasions and the fact that Beijing is currently stressing the improvement of its air and naval power projection capabilities.

[21] Taiwan's defense budget fluctuates between $8-$10 billion, while the PRC defense budget is generally estimated by most well-informed analysts as somewhere in the range of $30-35 billion. Moreover, due to the increasing cost of social welfare programs and infrastructure investment, the share of Taiwan's defense budget as a percentage of both total government expenditures and GDP has fallen in recent years. And much of Taiwan's defense budget is taken up by huge personnel costs, which greatly exceed both operational costs and military purchases. In the FY99 defense budget, these three categories of expenditure respectively accounted for 50.5%, 19.09%, and 30.86%. Moreover, arms acquisitions represent only a very small portion of overall military purchases. See Ding and Huang paper, pp.2-3.

[22] In recent years, however, a greater emphasis has been placed on developing joint operations capabilities. Specifically, efforts to develop joint operations have made some significant headway in the areas of C3I and EW / reconnaissance, where jointness is becoming increasingly necessary. For further details, see Swaine, 1999.

In recent years, however, military planners and political leaders have placed an increasing emphasis upon the development of a more robust military deterrence, in response to the growing capabilities of the PRC. For most observers, this shift in emphasis implies a focus on the acquisition of a capable air and missile defense system and a significant number of surface and subsurface naval assets, to deal with the threat to Taiwan's security posed by the growing possibility of air or missile displays or attacks, naval harassment or blockades, and amphibious and air-based invasions of territory under ROC control. The Democratic People's Party under the leadership of President Chen Shui-bian, however, has also sought to move Taiwan's strategy from its purely defensive focus to incorporate more tactically offensive and counterattacking elements.[23] On 16 June 2000 at 76th anniversary of the Chinese Military Academy in Gaoxiong, Chen re-introduced the concept "decisive offshore battle" or "decision campaign beyond boundaries" (*jingwai juezhan*), which had first appeared in the DPP White Paper in November 1999. Almost immediately, Chen's doctrine encountered heavy military resistance, particularly among officers who suspected that the strategy reflected an intention to take the fight to the mainland. To counter these criticisms, Taiwan government officials over the course of the latter half of 2000 and the first months of 2001 have repeatedly offered differing definitions and articulations of the strategy, and the operationalization and implementation of the concept still appears ill-formed.

To better understand these new strains of offensive-oriented thinking and their possible policy trajectories, it is useful to examine some of the DPP's cornerstone policy documents. In its "policy manifesto," the DPP asserts that Taiwan "must maintain an efficient yet credible deterrence force to preempt any belligerent action towards Taiwan."[24] The focus on deterrence rather than defense is an important signal of the break with the immediate past, especially the early years of the Lee Teng-hui regime when defense enjoyed the top priority. The DPP instead clearly seeks to move the battle away from the island:

> Our military strategy should be adjusted from passive to aggressive defense. We should abandon the idea of beachhead operation and replace attrition combat with operations to paralyze the enemy. We need to acquire the ability to disable the enemy from starting a war against us, so as to avoid fighting a war on our own soil and avoid endangering the people's lives and property.[25]

Thus, the goals of this strategy are to acquire the capability to "push" Taiwan's defense deep and wide into enemy territory, thus increasing deterrence, paralyzing the enemy's ability to make war on TW, and avoiding losses on the Taiwan side.

Yet the advocates for this position are also adamant that Taiwan will never fire first, despite the attractiveness of pre-emption for achieving these goals.[26] They point out that Taiwan has never felt the need to pre-empt historically, though this may have been largely predicated on US intervention. While not firing first, there is consensus that Taiwan must quickly seize the

[23] This section benefited heavily from Alexander Huang's excellent essay "Homeland Defense with Taiwanese Characteristics: On President Chen Shui-bian's New Defense Concept," presented at the 11th Annual PLA Conference, U.S. Army War College, Carlisle Barracks, PA, 1-3 December 2000.

[24] "DPP Year 2000 Policy Manifesto Abstract," 24 November 1999.

[25] Democratic Progressive Party Policy Committee, "White Paper on Defense," 23 November 1999.

[26] In November 2000, Defense Minister Wu Shih-wen asserted "We would never be the first to fire." See "Taiwan Defense Budget Drops to New Low," *Central News Agency*, 20 November 2000.

initiative from their attacker, although the line between pre-emption and immediate counterattack is sometimes blurred. This gray area is highlighted by Alexander Huang, who argues:

> Based on Chen Shui-bian's campaign platform, Taiwan would not engage in arms conflict with the mainland until deterrence fails. In other words, once PRC initiates a war or shows it is preparing to use force, Taiwan will have the rights to conduct attack targets on the mainland.[27]

Since Chen's official announcement of "decisive campaign beyond boundary" in June 2000, some defense advisors within the DPP conducted an assessment on the legality of "anticipatory self-defense" in international law, analyzing the blurred line between first strike and second strike,[28] the feasibility of preemptive air strike against the mainland,[29] and other theoretical studies. If it can be verified that the PRC intends to attack, they reportedly concluded that it is not entirely illegal under international law to strike first.

Assuming that the PRC does strike first, Taiwan's response options are discussed under the single rubric of *fanzhi*, or "counterstrike."[30] The plan is to survive the first strike through hardening and civil defense, and then conduct a counterstrike. However, there is significant debate within Taiwan about the exact purpose of this counterstrike. All interlocutors agreed that it should be designed to qualitatively degrade Chinese capabilities, though there were two views of the end game. A more aggressive group spoke of the counterstrike as the end game itself, presumably a military "victory" with no political negotiation, while another group saw the purpose of counterstrike as primarily improving Taiwan's position at the negotiating table with the Chinese. The counterstrike itself would involve "decisive action" to destroy any enemy force before it enters our territory, preferably destroying the enemy deep in its own rear base and paralyzing the military targets on its soil." Guided by the aphorism that "offense is the best defense," the DPP Defense White Paper asserts that "every military target and facility of the enemy that pose a threat to us will be on our list of targets of attack, and we will take immediate and effective countermeasures which may include preemptive measures to effectively destroy or disable the enemy's war machine."[31] Specifically, Taiwan's armed forces would seek to use information superiority, air superiority, and long-range precision strike to destroy the enemy's C3I system, logistics capacity, and assembly areas. These capabilities would be achieved through the use of "long-range, precision, guided weapons" and information warfare. Missiles in particular would "make accurate strikes deep into enemy territory and put the enemy's most threatening, key political and military targets well within range."

Since Chen's elections, these DPP defense policies have been partially implemented, though resistance from the military has been palpable. The first challenge for officials was providing a

[27] Alexander Huang, "Homeland Defense with Taiwanese Characteristics: On President Chen Shui-bian's New Defense Concept," presented at the 11th Annual PLA Conference, U.S. Army War College, Carlisle Barracks, PA, 1-3 December 2000.

[28] Su Tzu-yun, "The Feasibility of Making First Strike and Taiwan's Rights of Anticipatory Self-Defense," conference paper for Air War College Conference on *Air Force 2011*, November 4, 2000, pp. 3-2, 3-17.

[29] Chang Kuo-cheng, "On the Execution of Air Operations Beyond Boundary," paper presented at the Air War College Conference on *Air Force 2011*, November 4, 2000. Mr. Chang is deputy director of DPP's China Affairs Department and was special assistant to the Vice Minister of Defense Dr. Peter Pi-chao Chen.

[30] At least one interlocutor objected to the "newness" of this idea, claiming that Taiwan has always seemed to have had a tactically offensive doctrine.

[31] Democratic Progressive Party Policy Committee, "White Paper on Defense," 23 November 1999.

concrete definition of "decisive offshore battle," which seemed at variance with the MND's stated policy and the articulated doctrines of the ground, air and naval forces. During his brief tenure as Premier, former Defense Minister and Chief of the General Staff Tang Fei reportedly had reservations about "decisive offshore battle" term, but agreed that any defensive war should be kept away from the island.[32] The current Chief of the General Staff Tang Yaoming and Defense Minister Wu Shih-wen have also made public statements in the summer of 2000 that seemed to move slightly toward the idea of decisive offshore battle, with Tang Yaoming conceding that the military's strategy need to move "a little offshore."[33] General Tang Yaoming asserted that "decisive offshore battle" is by no means an offensive strategy, since "it does not mean that we will launch an attack on mainland China. We neither have such a capability at the moment, not have we any such development plan. We have no plan to develop surface-to-surface missiles – an effective offensive weapons."[34] Instead, the gist of "decisive offshore battle" is "foiling invading mainland Chinese forces at sea or in the air over the Taiwan Strait by using joint forces of all military branches and avoiding bringing war to Taiwan and its outlying islands."[35] Beginning from the premise that Taiwan is in a "defensive position and has no initiative whereas the enemy has the initiative in war,"[36] Minister Wu advocated a similar interpretation of "decisive offshore battle":

> Fighting a 'decisive offshore battle' means that we should not let the flames of war spread to our island or our land. Offshore therefore refers to the Taiwan Strait. We will not necessarily solve the problem in the Strait to the west or the east of the central line of the Strait. The concept does not suggest an offensive operation, for an offensive operation would run counter to our present strategy of 'resolute defense' to a certain extent.[37]

Still, the MND has yet to adopt the term wholesale, preferring "source strike" to "decisive offshore battle." The former term sbows up in the Executive Yuan's newly approved mid-term administrative project proposals for 2001-2004, in which the MND specifies its future tasks as focusing on developing joint operations and "source strike capabilities."[38] The difference between "source strike" and "decisive offshore battle" may only be semantic, but perhaps it is significant that the Ministry continues to resist adopting the President's specific terminology.

While there does seem to be a growing consensus in favor of moving the battle off the beaches, there is still a great deal of debate over offensive operations on the mainland. The first official mention of the development of offensive systems occurred during former Chief of the General Staff Tang Fei's closed testimony to the Legislative Yuan on 15 April 1999, though a military spokesman immediately denied the remark.[39] In examining the motivation for a shift to offense, two rough schools of thought can be identified. The first argues that the acquisition of an

[32] Cheng-yi Lin, "The Security of Taiwan in the Year 2000: A Taiwanese Perspective," unpublished paper.

[33] Sofia Wu, "Military Chief Explains 'Offshore Defense' Concept," *Taipei Central News Agency*, 7 July 2000.

[34] Sofia Wu, "Military Chief Explains 'Offshore Defense' Concept," *Taipei Central News Agency*, 7 July 2000.

[35] Sofia Wu, "Military Chief Explains 'Offshore Defense' Concept," *Taipei Central News Agency*, 7 July 2000. See also *Qingnian ribao* [Youth Daily News], 8 July 2000, p.3.

[36] Huang Ching-lung, Kuo Chung-lun, Hsia Chen, Lu Chao-lung, and Wu Chung-tao, Defense Minister Wu Shih-wen Says: The Nationalist Forces Now All Know that President Chen Will Not Stand for Taiwan Independence," *Zhongguo shibao*, 2 July 2000.

[37] Huang Ching-lung, Kuo Chung-lun, Hsia Chen, Lu Chao-lung, and Wu Chung-tao, Defense Minister Wu Shih-wen Says: The Nationalist Forces Now All Know that President Chen Will Not Stand for Taiwan Independence," *Zhongguo shibao*, 2 July 2000.

[38] "Air Force to Introduce New Strategies," *China Post*, 27 December 2000.

[39] Lu Te-yun, "Taiwan to Develop 'Offensive Weapons'," *Lianhebao*, 16 April 1999, p.1.

offensive counterforce capability is necessary to deter China from launching a conventional attack against Taiwan, and if deterrence fails, to significantly degrade China's ability to sustain such an attack against Taiwan. These forces would consist essentially of several hundred short-range ballistic missiles (SRBMs), air assets, and possibly even a LACM variant of the Hsiung-Feng II capable of striking China's ports, theater C3I nodes, and missile launch sites. The second group argues that Taiwan must focus on acquiring offensive strategic countervalue capabilities to threaten major Chinese cities in Central and Southern China, such as Shanghai, Nanjing, Guangzhou, and Hong Kong. These would consist essentially of a relatively small number of intermediate-range ballistic missiles (IRBMs) or medium-range ballistic missiles (MRBMs) with large conventional or perhaps even nuclear or biological warheads, intended purely as a deterrent against an all-out Chinese assault on Taiwan. After former President Lee Teng-hui put forward his controversial "special-state-to-state" (*liangguolun*) formulation, KMT party stalwart and KMT, Inc. bagman Liu Taiying threatened that Taiwan would conduct a surprise missile attack on Hong Kong and the open seas off Shanghai if the mainland used force.[40] Both schools recognize that the success of the effort requires significant enhancement in the hardening of the island, including both active defenses and passive defenses. To this end, the MND claims that the majority of Taiwan's military facilities and weapons depots have been moved underground to avoid possible mainland Chinese attack. The military is also using separation and camouflage strategies to hide or disguise its facilities and installations.

Alexander Huang identifies four counterarguments offered by opponents of this new, offense-oriented mindset.[41] First, international reaction will likely be negative. Analysts argue that it is extremely unwise to "talk" too much about Taiwan's offensive options, especially before acquiring such a capability. A clear pronouncement of the intention of taking preemptive actions against the PRC would be "politically devastating to Taiwan, because it will unnecessarily provoke Beijing and antagonize Washington." Second, "without sufficient deterrents in Taiwan's inventory, Chen's concept would naturally lead to a suspicion in the international community that Taiwan may eventually for a nuclear option." Third, no one can outline the exit strategy [*zhongzhan zhidao*] for these options. Fourth, the DPP failed to analyze whether Taiwan would be able to acquire the technologies to implement this new strategy, and failed to weigh the domestic and foreign costs of pursuing such a line. An additional criticism of the countervalue strategy would highlight the vulnerability of the Taiwan missile infrastructure, and the difficulty of achieving deterrence with a limited number of airframes.

Taiwan's Military Strategy and RMA Policies

From both official and unofficial statements, the Taiwanese military seems committed to the RMA. As early as 1996, the Ministry of National Defense White Paper called for RMA-related modernization efforts in all three services. The Army in particular was directed to strengthen its electronic warfare capability and upgrade its C3I system, while the Air Force was focused on photo-reconnaissance, early warning, and electronic warfare planes.[42]

[40] Chen Shi, "Taiwan: Is It Useful to Develop Offensive Weapons?" *Zhongguo qingnian bao*, 24 December 1999.

[41] Alexander Huang, "Homeland Defense with Taiwanese Characteristics: On President Chen Shui-bian's New Defense Concept," presented at the 11th Annual PLA Conference, U.S. Army War College, Carlisle Barracks, PA, 1-3 December 2000.

[42] Nien Chen, "An Analysis of the 1996 Republic of China Defense White Paper," *Ch'uan-Ch'iu Fang-Wei Tsa-Chih* [Defense International], 1 July 1996.

Between 1996 and 1999, the emphasis on RMA developments increased significantly, driven in part by the personal advocacy of General Tang Fei and the interest of the opposition Democratic People's Party in future warfare. In its 1999 Defense White Paper, the DPP declared that "the Taiwan military should actively develop electronic information combat capacity, and amplify the C4ISR system to ensure our information superiority in the Taiwan Strait."[43] Moreover, they declared that the focus of MND modernization should be the Navy and the Air Force, not the traditionally favored ground forces.[44]

The DPP's proscribed military strategy included the principle "Strike Deep and Wide," which incorporated many aspects of U.S. command and control warfare (C2W). According to this strategy, some of which has been formally proposed since the DPP assumed the presidency, the Taiwan military should focus its energies on developing an information warfare capability, as well as long-range, precision, guided weapons. In peacetime, this information superiority, command of air space over the Taiwan Strait, and long-range, precision guided strike capability would be used to maintain a strong deterrence force in peacetime. In wartime, such assets could be used to seize immediate information superiority and air and sea command in the Taiwan Strait to inhibit and destroy the enemy's command and information system and sea and air combat and logistic supply capabilities. In addition, the DPP report called for the development and deployment of long-range early warning radar and unmanned reconnaissance vehicles, as well as military surveillance satellites to increase Taiwan's early-warning capability.

The 2000 Defense White Paper issued by MND represents the apex of RMA-directed policies thus far. In its opening paragraphs, the report declared:

> The Revolution in Military Affairs (RMA) is a worldwide trend in military development. The Republic of China's Armed Forces should also follow the trend to promote the RMA.[45]

Reflecting a maturing understanding, the report specifically broadened the definition of revolutionary trends to include not only technology, but also advanced concepts, technological know-how, and organizational structures. In particular, the report highlighted the extent to which technical innovation is producing profound effects, particularly in regard to precision strike, dominant maneuver, space operations, and information warfare. The last sector received special emphasis in the document, which asserted that "the buildup and enhancement of cyber warfare capability for offensive/defensive operations and related defense technologies will safeguard the nation's security.[46] To meet the challenges of communication and information threat from the enemy and to establish this fighting capability in information warfare, the White Paper's recommendation was four-fold: (1) to build a defense information infrastructure (DII); (2) to develop a C4ISR infrastructure; (3) to augment security measures; and (4) and to develop offensive information warfare capabilities. Each of these efforts is discussed in more detail in later sections.

[43] Taipei Democratic Progress Party (DPP) Policy Committee, "White Paper on National Defense," 23 November 1999.

[44] Taipei Democratic Progress Party (DPP) Policy Committee, "White Paper on National Defense," 23 November 1999.

[45] 2000 White Paper.

[46] 2000 Defense White Paper.

More recent comments by President Chen Shui-bian and Defense Minister Wu Shih-wen confirm the trend towards the development of RMA-related programs in the Taiwan military. At the 75th anniversary ceremony for the Armed Forces University in June 2000, President Chen Shui-bian identified "upgrading early warning and electronic warfare capabilities" as a main direction for future military build-up and combat preparedness training.[47] In July 2000, Defense Minister Wu highlighted continuing efforts in modernizing the C4I infrastructure, pressing the point that Taiwan need to build "a really integrated telecommunications system for our three services."[48] Expanding on these remarks, Wu in February 2001 asserted that the armed forces would take advantage of military and private sector fiber-optic, wireless, and fixed line communication systems to create a multi-conduit system that uses national resources effectively, with a particular focus on "information protection."[49] Moving from defense to offense, however, Wu also highlighted the Taiwan military's continuing efforts to operationalize an information warfare unit capable of offensive operations as a core effort in developing a future RMA military.

Taiwan's Military Organization and the RMA

Advocates of the RMA often assert that the revolution is as much organizational as it is technological, since new strategies and weapons require fundamentally new forms of military structure. To this end, Taiwan's defense policy also includes efforts to streamline, restructure, and strengthen the organization of the ROC military, in order to ensure more effective civilian control over the armed forces, to more effectively integrate defense planning with the larger priorities of the government's national security policies, to eliminate waste, corruption, and inefficiency in military procurement and readiness, and to increase the military's overall combat effectiveness. These goals are to be accomplished largely through the promulgation and implementation of an extensive set of organizational reform laws and military restructuring programs.[50]

The most important of these laws is the landmark January 2000 National Defense Law (*Guofangfa*).[51] Its mandated changes affect nearly every level of the military, including lines of authority, numbers of personnel, strategic planning, and ratios of civilian and military personnel in the Ministry of National Defense. The reforms are seen by many as essential to improving the overall capability of the Taiwan military. At the same time, even advocates of the changes are attuned to bureaucratic reality, and are therefore implementing the measures in a phased approach.

One of the most important changes is an augmentation of the role of the Ministry of National Defense. The January 2000 National Defense Law eliminates the current direct link that exists, regarding operational matters, between the Chief of the General Staff and the president. In its place, the new National Defense Law combines the military administration and military

[47] Sofia Wu, "Chen Shui-bian Addresses Military Cadets; Urges Loyalty, Defense To Counter PRC," *Taipei Central News Agency*, 16 June 2000.

[48] Huang Ching-lung, Kuo Chung-lun, Hsia Chen, Lu Chao-lung, and Wu Chung-tao with Defense Minister Wu Shih-wen: "Defense Minister Wu Shih-wen Says: The Nationalist Forces Now All Know that President Chen Will Not Stand for Taiwan Independence," *Zhongguo shibao*, 02 July 2000.

[49] Fang Wen-hung, "Taiwan To Complete Military Restructuring in 3 Years," *Taipei Central News Agency*, 7 February 2001.

[50] See Swaine 1999, for details.

[51] The *Guofangfa* superceded the 1970 Organic Law of the Ministry of National Defense.

command systems into one and designates the minister of national defense as responsible for both systems.[52] This change would thus place the military and specifically the CGS *entirely* under the institutional authority of the MND and may thereby increase the ability of the MND to direct important aspects of defense policy. The CGS would serve as both the military staff for the Defense Minister and commander of military operations under the Defense Minister's supervision. Hence, this revision in the National Defense Law would also expose the CGS to greater legislative oversight, as a leading official of the Executive branch solely under the direct authority of the premier. Other proposed changes would reportedly place the service headquarters directly under the command of the MND and also greatly increase the number and functional expertise of MND offices. If enacted into law, these changes, combined with the convergence of military authority systems under the MND, could significantly shift control over basic military decisions from the GSH to the MND.

A second major reform involves the streamlining of the existing Taiwan military force structure. While the implementation of this reduction was initiated before Chen's election, the DPP in the past has been a strong advocate of streamlining and will likely aggressively pursue the implementation of the measures. The primary motivation for the DPP's support of reductions is financial, believing that streamlining will free monies for the purchase of high tech weapons needed for the Air Force and Navy to hold enemy forces away from the island. In the eyes of DPP experts, the first target for downsizing should be the ground forces, which are bloated in size and not central to the new, forward-leaning strategy.

Yet there is some debate over the target personnel level for the armed forces. In 1997, the armed forces stood at 450,000 personnel. According to Defense Minister Wu in February 2001, the ROC military will complete a major structural reorganization within three years and streamline itself to a target force of 350,000 soldiers by the end of 2006. The first phase of the three-staged modernization program will be finished by 30 June 2001, reducing the force to 386,000 soldiers.[53] The headquarters of the Ministry of National Defense was particularly hard-hit by the reorganization, reducing its staff by more than 27.9%.[54] Even after completion of the reform package in 2001, however, the army will still makes up 51.75% of the forces, compared with 14.61% for the ROCN and 14.33% for the TAF. One DPP legislator on the LY Defense Committee has called for reductions as low as 260,000, but the Ministry of National Defense maintains that the downsizing should be more gradual.[55]

The third set of reforms centers on strategic and policy planning within the military services, the "joint" staff, and the Ministry of National Defense. One historical barrier to the modernization of strategic planning has been the lack of true jointness in the Taiwan system. In terms of jointness and long-range planning, the institutions are still pretty weak. There is an office in the MND that combines the role of inspector general and joint doctrine, though it is really more focused on operational matters like common radios and common equipment. The J3 does some planning, but they reportedly don't have real plans. The most important office is the newly merged J5/*liandubu* office under Admiral Alan Hung in the Ministry of National Defense. This new combined office will have many functions, including day-to-day operations, international security affairs, and

[52] Cheng-yi Lin, "The Security of Taiwan in the Year 2000: A Taiwanese Perspective," unpublished paper.
[53] Fang Wen-hung, "Taiwan To Complete Military Restructuring in 3 Years," *Taipei Central News Agency*, 7 February 2001.
[54] 2000 White Paper, Part 6.
[55] Philip Finnegan, "Taiwan's Hopefuls Diverge on Defense," *Defense News*, 13 March 2000.

longer-range strategic planning. According to interlocutors, the first step in the latter effort will be strategic force planning, involving input from outside sources. Eventually, the office reportedly wants to outsource this work completely to civilian contractors. In terms of interoperability with the US during a crisis, there is also a special office under the J3, headed by Cheng Shiyu and called the *lecheng jihua*, that is exploring the topic.

In addition to these organizational reforms, a number of RMA-oriented institutions have emerged. The first is the Communications Electronics and Information Bureau, which is the coordinating institution within the Taiwan military for C4I, information warfare, electronic warfare, and other related areas. CEIB closely coordinates with the Chungshan Institute of Science and Technology, which is the central R&D center for the Ministry of National Defense. The Chungshan Institute of Science and Technology (CSIST), established in 1968, is the leading institution for the research, development, and design of defense technology in Taiwan. With its headquarters in Lungtan, Taoyuan County, the CSIST has facilities stretching over nearly 6,000 acres scattered throughout Taiwan, employing more than 6,000 scientists and 8,000 technicians. The institute itself is divided into four major research divisions: aeronautics, missiles and rockets, electronics, and chemistry. In addition, CSIST has six centers for systems development, systems maintenance, quality assurance, materials R&D, aeronautic development, and missile manufacturing. CSIST jointly conducts independent research and development of weapon systems with the Aero Industry Development Center, which is now under CSIST supervision; some manufacturing units of the Combined Services Force; academic institutions; and public and civilian industries. To date, a number of weapon systems have been domestically designed, tested, and produced on a mass scale by the CSIST. These include the Kung-feng 6A rocket, the Hsiung-feng I and Hsiung-feng II SAMs, artillery fire control systems, naval sonar systems, naval electronic warfare systems, and the Tzu-chiang trainer aircraft. The CSIST has produced or plans to produce Tien-kung (SKYBOW) I and Tien-kung II SAMs, Tien-chien (SKY SWORD) I and II AAMs, Hsiung-feng III cruise missiles, and Lei-ting (Thunderbolt) 2000 multi-barrel rockets.[56] Any future indigenous development of RMA technologies, or the integration of imported systems, will be carried out under CSIST's direction.

Military Modernization and the RMA

To successfully implement its new, more offensive-oriented military strategy, Taiwan must augment its limited indigenous military systems by obtaining critical weapons, support infrastructure and military technology and training from the outside. For more than a decade, Taiwan's military modernization effort has focused on acquiring modern weapons systems and associated equipment to deter--and, if necessary -- defeat Chinese aggression.[57] Billions of dollars have been spent on domestic programs like the Indigenous Defense Fighter (IDF) and the Tien Kung air defense system, as well as on foreign purchases like the U.S.-made F-16 fighter and the French-built Lafayette-class frigate. Many of these newer systems are in the process of being assimilated into the active inventory.

At the same time, however, Taiwan has actively pursued research and development of advanced RMA-related technologies. According to the 2000 Defense White Paper, Taiwan’s military R&D

[56] Peter Yen, "Diversification And Defense Trade Opportunities," U.S. Department of State, September 1999.

[57] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

is meant to focus on electronic battle, air and sea superiority, and anti-landing capability. Three key areas are electronic warfare, C4I modernization, and information warfare.

Electronic warfare

The first RMA area in which the ROC military expressed an interest was electronic warfare. In the mid-1990s, military programs centered on defensive uses of EW, particularly in air, sea, and ground operations.[58] Interest in EW has increased in recent years, thanks to greater PRC interest in acquiring electronic warfare equipment, advanced radars, airborne early warning aircraft, maritime surveillance radars, and anti-radiation missiles. In May 1999, Defense Minister Tang Fei testified that mainland China would likely attain an electronic warfare supremacy against Taiwan by 2010.[59] At the time, he noted that Taiwan had established a military task force to ensure the nation is prepared for electronic warfare. The task force is conducting relevant research and working out preventive measures against an enemy's electronic attack. Soon after, General Lin Chin-ching of the CEIB confirmed Taiwan's vulnerability:

> As to the overall threat, Taiwan's electronic warfare capability remains inadequate. The ROC military has established some electronic warfare capability, including information reconnaissance, defense and electronic strike, with aircraft- and ship-based self-defense electronic warfare capability being its main preparations. In addition, since it is lacking in all other areas, such as electronic parameter intelligence data analysis capability, battlefield electromagnetic spectrum management, anti-satellite reconnaissance, electromagnetic pulse defense, and jamming of enemy precision-guided attack weapons capability, it has included all of these in its planning preparations.[60]

According to the 2000 Defense White Paper, current efforts are devoted to improving communication countermeasures, electronics counter-countermeasures, developing opto-electronic countermeasures and early warning capability, as well as assisting the Armed Forces in the installation of training and testing of equipment.

C^4I modernization

Taiwan's military C4I system reportedly consists of a nationwide network of fixed telephone lines (coaxial and fiber optic) and microwave, as well as satellite, troposcatter and HF/VHF radio. The Taiwan military is currently involved in an active program of C4I modernization. General Tang Fei, former Chief of the General Staff and Defense Minister, is widely credited with emphasizing the importance of this sector, which previously had not enjoyed the same level of priority as higher-profile political programs involving U.S. arms sales. Perhaps the most important period in this process was the U.S.-Taiwan military exchanges on battle management and C4I in 2000, which identified key problems in the system and put forward a set of operational recommendations. The current Defense Minister Wu Shih-wen and Chief of the General Staff Tang Yao-ming have publicly endorsed these recommendations.

[58] "On EW and C3I's Role in Taiwan Defense," *Fang-wei Ta Tai-wan*, 1 November 1995, pp.354-361.

[59] "Tang Fei: PRC May Have Electronic War Supremacy by 2010," *Taiwan Central News Agency*, 05 May 1999.

[60] Lu Teh-lin, "Faced with the PRC Information Warfare and 'Electronic Warfare' Threat, Lin Chin-ching Says that Taiwan's Electronic Warfare Capability Remains Inadequate," *Lianhebao*, 15 September 1999.

Communications. In May 2000, Taiwan’s Sixth Field Army formally completed the installation of the Improved Mobile Subscribe Equipment (IMSE) system, whose technology is based on the US Army's currently deployed MSE system. For the Taiwan Army, this communications system forms the backbone of the ROC Army's move toward digital battlefield technology.[61] The IMSE system uses UHF, VHF, and SHF communication frequencies to send encrypted data through a series of midpoints housed in mobile all-terrain vehicles. It is capable of providing telephone, voice, digital, and fax services within the system or in tandem with private sector telecommunications systems. For advocates, the ability of IMSE to deploy anywhere and to transmit encrypted digital battlefield intelligence data makes it the indispensable backbone to a futurized battlefield neural network. Each of the ROC Army's higher capacity IMSE transfer points, designed for the division level, can connect 120 voice and 124 digital users, while smaller capacity transfer points can provide combined brigade and battalion-level service to 40 voice and 63 digital users.[62] IMSE showed its operational value during the major earthquake that hit Taiwan on 21 September 1999 and shut down major power grids and telecommunications links in central Taiwan. According to press accounts, Army Commander-in-Chief Chen Cheng-hsiang ordered the 63rd Communications Group's 712nd Battalion to assist in the immediate recovery of the communications system in the Chichi area. Vehicles carrying components of the IMSE system set up the network in the disaster area, and all telephone calls to and from the region were routed through the system during the period after the quake struck. The success of the IMSE system during the earthquake has led to a proposed acquisition of a second-phase system, though this procurement is currently facing opposition from the other services as well as legislators seeking to encourage indigenous production at CSIST.

In January 2000, the Taiwan military entered a new period of military communications when it completed a broadband fiber optic cable communication network connecting the Hengshan Command Center in Taipei with frontline combat units.[63] Vice Chief of the General Staff Gen. Miao Yung-ching presided over the inauguration of the Armed Forces Fiber-optics Communications System in May 2000, saying that the system will give the armed forces the ability to "hear, see, and command."[64] The newly completed fiber-optics communication system will allow the defense ministry to acquire near-instantaneous audio-video intelligence from the frontlines and conduct operational meetings with its field commanders through videoconferencing. Miao noted that as military components continue to be consolidated after the streamlining of Taiwan's new-generation armed forces, systems that provide enormous firepower need a precise intelligence and information gathering system together with a communications

[61] Wen-Hung Fang, "Taiwan Army Equipped With Digital Battlefield Communications System," *Taipei Central News Agency*, 13 May 2000.

[62] Based on the success of this system, the army in late 2000 still wished to buy a second unit of IMSE, estimated to cost more than NT$25 billion.[62] An army official was quoted at the time as saying: "The system is the best tactical communications system we have had in decades. We really need it to build a nationwide battlefield communications network for the best survivability and maneuverability in war." Yet the proposed purchase of the system encountered intense opposition from the other armed services and lawmakers in the Legislative Yuan. LY members complain that the system's overly strong power might affect civilian wireless communications. Additional criticism was offered by KMT lawmaker and defense committee member Chou Cheng-chih, who led the move against the deal on the grounds that the Chungshan Institute should be permitted to develop a domestic alternative. Other services in the military voiced opposition to the project, saying that the army's efforts to build its own C4ISR (command, control, communication, computer, intelligence, surveillance and reconnaissance) system on the basis of the communications network are beyond its ability.

[63] “Taiwan Armed Forces to Test Cable Network in War Games,” *Central News Agency*, 3 January 2000.

[64] Wen-Hung Fang, "Taiwan Military Using Fiber-Optic Communication System," *Taipei Central News Agency*, 26 May 2000.

system that can deliver such intelligence and relay operational orders. He said that intelligence departments in the future will no longer have to use "special couriers" because the fiber-optics network will be able to transmit broadband video, still pictures, and digital data, as well as traditional voice communications from the frontlines. Planning and designing of the system began in 1990, while installation of the fiber-optic cables and equipment, testing, and transfer to the new system began in June 1997, Miao added.

Reconnaissance Capabilities. During the 1980s, Taiwan's reconnaissance capability and 1970s vintage photographic technology was adequate for the limited capabilities and low threat posture of the PLAAF. Taiwan's airborne reconnaissance capability, however, began to decline precipitously in the 1990s. Last year, the TAF retired the last of its RF-104G tactical reconnaissance aircraft and replaced them with reconnaissance-configured RF-5E aircraft. Taipei continues to seek a new imaging system capable of exploiting targets at greater distances from the coast, but without exposing its reconnaissance flights to China's increasingly more sophisticated air defenses. Taiwan conducts technical and human intelligence operations against China and purchases French SPOT, U.S. LANDSAT, and possibly U.S. IKONOS II commercial imagery for exploitation.[65] Finally, research is currently being conducted on tactical unmanned aerial vehicles (UAVs), which can be used for day-and-night reconnaissance photography, real-time information transmission, automatic pilot control, and global positioning navigation.[66]

STRONG NET radar. Taiwan’s original air defense radar network was known as SKY NET.[67] Its replacement, known as STRONG NET, is based on a system of 35 radars on 21 radar stations, and can identify aircraft within a range of 600km (370 miles).[68] The network was reportedly upgraded in the mid-1990s at the cost of US$100 million.[69] By 1998, the Strong Net system could reportedly utilize the early warning radar from the E-2T plane to integrate naval vessels, army missiles, and the air force defense-artillery system to form a complete air defense network, eliminating the “dead space” problem with the land base radars and maximizing overall air defense effectiveness.[70] In addition, the air defense weapons of the three services are incorporated into the system, using a flexible communications network for direct operations command. In late 1999, press accounts Taiwan is spending over 5 billion NT dollars to upgrade STRONG NET for more advanced air intelligence monitoring and C2 for joint aircraft, missile, and AAA air defense of Taiwan, the Penghu's, Quemoy, and Matsu.[71]

Long-Range Early Warning Radars. In the late 1990s and 2000, early warning radars appeared on Taiwan’s procurement shopping list. Taipei’s official policy views on the matter were revealed in March 1999, when Air Force Deputy Chief of Staff Wang Chih-ke confirmed that purchasing an early warning radar was “the policy of the Defense Ministry.”[72] The main

[65] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

[66] 2000 White Paper.

[67] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

[68] General Confirms Policy on ‘Long-Range’ Radar,” *AFP*, 23 March 1999.

[69] Yuan Lin, “The Taiwan Strait is No Longer a Natural Barrier – PLA Strategies for Attacking Taiwan,” *Kuang Chiao Ching*, 16 April 1996.

[70] Liu Yun, "A Tight Encirclement -- Escape is Impossible, Even with Wings," *Sheng-li Chih Kuang*, 1 April 1998, No.520, pp.18-22.

[71] Zhu Xianlong, "Taiwan's Air Defense Capability in Perspective," *Ta Kung Pao*, 12 September 1999, p.B2.

[72] General Confirms Policy on ‘Long-Range’ Radar,” *AFP*, 23 March 1999.

rationale for the long-range early warning radar centers on the Chinese missile threat and Taiwan's hope to deploy theater missile defenses. The TMD argument for the radars has both political and military dimensions. On the political front, additional early warning of Chinese missile attack is seen as a civil defense measure and a boost to public morale, particularly if it improves the population's chances of survival. On a military level, early warning radar is perceived by advocates in Taiwan and Washington as aiding peacetime monitoring of Chinese air deployments, missile engagement, and dispersal of forces, as well as leadership survival. The radars do offer some ability to track aircraft, but the high rates of commercial air traffic in the area and the curvature of the Earth are constraints.

One obstacle in the procurement process was choosing the appropriate radar. Early on, there was discussion about selling PAVE PAWS to Taiwan, but there was general agreement that such a powerful radar far exceeded the needs of Taiwan, especially given its lack of strategic depth. Instead, Washington conducted studies to determine the island's actual requirements, in order to construct a custom-configured set of radar systems to meet those specifications. Interlocutors in Taiwan describe a system of strategic and tactical radars, with two giant phased-array radars at the north and south ends of the island connected by a set of smaller radars at the sites of missile batteries and other TMD infrastructure. By one estimate, the new radars alone, including perhaps two strategic early warning radars and a network of tactical radars, could cost NT$26 billion (US$785.7 million).[73] There are reports that this plan has already been approved, though there is no evidence that Taiwan has allocated money to purchase the systems. Given the political support for the transfer, however, it seems certain that the radars will be acquired and deployed as soon as possible.

Airborne Early Warning. Taiwan currently possesses four E-2C aircraft, renamed E-2T for export to the island. The custom-designed configuration does not include all of the electronics packages found in the American variant. Since 1990, for example, American E-2C planes have been equipped with the much improved AN/APS-145 radars. However, the E-2T's Taiwan are still equipped with AN/APS-138 radars developed in 1983, which are inferior in performance. It is also reported that, for security reasons, the Americans have removed some important "modules" from the planes, including IFF codes and data links. In May 1998, the US reportedly changed its previous policy of rejecting Taiwan's request for purchasing data links, agreeing to provide Taiwan with data link systems to facilitate communications among Taiwan's F-16s, E2T early warning/command aircraft and warships.[74] These links were reportedly sold in May 2000.[75]

Information warfare

Perhaps the most important future RMA capability for the Taiwan military is information warfare, particularly computer network operations. Taiwan military and civilian leaders since the late 1990s have increasingly identified IW as a core interest. During his presidential campaign in 1999, for example, Chen Shui-bian argued that Taiwan should build "information warfare

[73] The money for the long-range radars was approved in the LY, after an intense dispute over the money for the land. The early warning radar alone is likely to require at least 6 years to IOC.

[74] Jay Chen and Sofia Wu, "US Reinforcing Military Software Exchanges With Taiwan," *Taiwan Central News Agency*, 24 May 1998.

[75] Sofia Wu, "US to Sell Taiwan Data Links for 2nd-Generation Warplanes," *Central News Agency*, 2 March 2000.

capabilities."[76] In November 1999, then Minister of National Defense Tang Fei submitted a National Defense Policy Report to the LY, emphasizing the central importance of information warfare as a new type of war and indicating his intentions to give top priority to IW-related preparations. In March 2000, the Taiwan military's head information warfare officer Lin Chin-ching publicly declared that "building up information warfare attack and defense capability is obviously the top-priority mission of our armed forces preparation."[77] Answering inquiries from legislators in November 2000, Lin continued this line of argument by asserting that IW would "become a key factor in the balance of power in the Taiwan Strait in the future," adding that then-Chief of the General Staff Tang Yao-ming wanted the military's future arms build-up to focus on [the creation of an IW force]."[78] Six months into his term, President Chen Shui-bian in December 2000 urged the military to further upgrade its information warfare capability and develop an integrated combined services command and control system.[79]

The main driver of Taiwan's interest in information warfare is the perceived growing threat posed by China's interest in information warfare. Advocates of information warfare in Taiwan note the dangerous IW asymmetry across the Strait, since Taiwan's economy, government and military are highly dependent on computers and could be vulnerable to such high-tech weapons. These attacks are potentially highly destabilizing to Taiwan, both for physical and psychological reasons. On the physical side, some believe that the PRC could use electronic and computer technologies to destroy or disrupt critical civilian and military infrastructure, including information and communications systems and military command structures, without much expense and loss of life.[80] But the psychological impact may even be more significant, as Chinese information warfare might bring about social confusion, undermine public morale, spread disinformation, paralyze the financial market, and thereby aid the PRC in successfully coercing the Taipei government to enter negotiations for reunification.

In the summer of 1999, these fears of Chinese IW attack appeared to be confirmed by substantial hacking from the mainland. The impetus for the attacks was then Taiwan President Lee Teng-hui's radio interview to a German news organization, Deutsche Welle in June 1999. In the course of his remarks, he put forward a controversial new formulation for China-Taiwan relations, which he dubbed "special state-to-state relations" (*Liangguolun*). Given the importance of subtle changes of language in the highly charged sovereignty conflict across the Taiwan Strait, Beijing's reaction to this new description was predictably intense. For weeks, both governments exchanged charges and countercharges, threats and counter-threats. The populations at large continued this ferocious debate on the Internet, creating nationalist web pages and exchanging epithets in Chinese-language chat rooms. It was not long before this war of words involved the hacker communities on both sides, and by early August a full-scale hacker war had erupted. The first salvo was actually a piece of psychological warfare that spilled over into the world of reality. On 6 August, a Chinese-language website registered in the United State but owned by a Chinese company posted a false news report that a Taiwanese F-5E fighter aircraft had been

[76] Chen Shui-bian, *Xinshiji xinchulu: Chen Shui-bian guojia lantu – diyice: guojia anquan* [New Century, New Future: Chen Shui-bian's Blueprint for the Nation – Volume 1: National Security], Taipei: Chen Shui-bian Presidential Headquarters, 1999), pp.50-51.

[77] Lin Chin-ching, "Comparison of PRC, ROC Information Warfare Capabilities," 1 March 2000, pp.68-73.

[78] Brian Hsu, "Taiwan Military to Establish Information Warfare Unit," *Taipei Times*, 23 November 2000.

[79] Sofia Wu, "Taiwan President Chen Urges Military To Further Upgrade Capabilities," *Taipei Central News Agency*, 30 December 2000.

[80] Lin Chin-ching, "Comparison of PRC, ROC Information Warfare Capabilities," 1 March 2000, pp.68-73.

downed by a Chinese Su-27.[81] The report sent the Taiwan stock market into a downward spiral, dropping nearly 2 percent in a single day.

This event was quickly followed by a rapid series of hacks of government and commercial Internet sites by hackers on both sides of the Strait. Some hacks were the work of individuals, while others represented the handiwork of loose groups of hackers with prosaic names like the "Alliance of Red Chinese Hackers" and the "Chinese Hackers Emergency Conference Center."[82] A partial list of these hacks is compiled in Table 1 below.

Table 1. Known Hacked Sites (partial list)

Country	Hacked Sites
China	Securities and Regulation Commission Science and Technology Commission Ministry of Railways Shaanxi Science and Technology Network Shanghai Huwan Education Bureau
Taiwan	Control Yuan Investigation Bureau National Assembly National Taiwan University Library Industrial Technology Research Institute Administration Government Information Office (Executive Yuan) Council of Labor Affairs Pingtung County Government National Information Infrastructure (NII) Project National Center for Research on Earthquake Engineering National Laboratory Animal Breeding and Research Center National Institute of Preventive Medicine Data Communication Business Group of Chunghwa Telecom Third and Eighth River Basin Management Bureau

On 9 August, a person claiming to be from the mainland and reportedly operating from a site in Hunan Province hacked into the website of the Taiwanese Control Yuan, the government's watchdog agency, and posted pro-China messages meant to refute President Lee's "special state-to-state" formulation.[83] One message inserted into the page read "Only one China exists and only one China is needed." Another message asserted that "The Taiwan government headed by Lee Teng-hui cannot deny it."

Taiwanese hackers retaliated by inserting pictures of Taiwan's flag, sound files that played the Taiwanese national anthem, and pictures of Taiwan's presidential candidates on mainland Chinese web sites.[84] They also posted statements on the web sites: "Reconquer, reconquer,

[81] "Taiwan Cites Internet Rumors," *Associated Press*, 7 August 1999.

[82] Sumner Lemon, "Hackers Keep Up Attack on Taiwan Web Sites," *Computerworld Hong Kong*, 24 August 1999.

[83] "Pro-China Hacker Attacks Taiwan Government Web Site," *Reuters*, 9 August 1999.

[84] "Taiwan Cyber-Hackers Strike Back at China," *Reuters*, 10 August 1999.

reconquer the mainland," "Counter the Chinese Communists," "Taiwan does not belong to China," and "Seriously, Taiwan is also better."[85]

As time went on, the attacks became more serious. On 10 and 12 August, a mainland hacker twice broke into the web site of the Taiwanese National Assembly, paralyzing its mainframe computer.[86] During the first attack, only files were replaced and a flag graphic was placed on the front page, but the second attack reportedly included the introduction of viruses into the system, thereby damaging both hardware and software.[87] Throughout the remainder of the month of August, both sides kept up the assault. At the height of the crisis, CCTV, China's main television station and reportedly a high priority target for Taiwanese hackers, claimed that its servers were being attacked once every three minutes. As August became September, however, the furor began to die down, and the hacker attacks dropped off correspondingly.

In retrospect, the hacker "war" between China and Taiwan involved a significant amount of activity on both sides, though none of it can currently be confirmed as state-directed computer network attacks. The Taiwan National Security Bureau, which is responsible for Internet security on Taiwan, reported that Taiwan suffered 72,000 "attacks" during the skirmish, those only 165 penetrations were successful.[88] The 72,000 figure must be treated with some caution, however, as it likely represents 72,000 "scans" of Taiwanese systems, hundreds or thousands of which could automated by a small group of people. There are no comparable figures for the Chinese side, though at least five penetrations could be confirmed. The vast majority of the attacks appear to be a form of "web vandalism," with young people defacing lightly protected external web servers of government offices. It cannot be discounted, however, that the military or security services on both sides of the Strait took advantage of this chaotic environment to conduct more sophisticated and malevolent computer network exploit activities.

In the aftermath of this incident, official estimates from Taiwan's Ministry of National Defense assert that China might be able to achieve this capability by 2005.[89] Pentagon estimates also suggest that China has yet to acquire an operational capability:

> Although the PRC has achieved certain results in information warfare tactics, their basic capability and technology in information science and technology is still at the elementary research and development stage. The major reason is that its domestic information industry is still mainly in re-processing manufacture and there is no real research and development capability to be mentioned.[90]

Analysts in both Taipei and Washington speculate that China's future cyber arsenal might include computer viruses and possibly even electromagnetic pulses (EMP) weapons.

[85] "Taiwan-China Hackers' War Erupts," *Muzi Lateline News*, 10 August 1999.

[86] Amanda Chang, "Beijing's 'Information War'," *Taiwan Central News Agency*. 12 August 1999.

[87] David Watts, "Virtual Warriors Fire Opening Shots in Cyber Battle," *The Times*, 18 August 1999.

[88] Michael Laris, "Chinese Web Warriors: Hackers in Taiwan, China, Trade Shots in Internet Skirmish," *Washington Post*, 11 September 1999.

[89] "Taiwan Prepares for Possible Chinese Cyber Attacks," *AFP*, 2 November 1999.

[90] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

Ironically, Taiwan appears to possess the greater potential to develop an operation information warfare capability, since its information technology sector is significantly more advanced than its counterpart on the mainland. Taiwan's possible advantages in this area have not gone unnoticed by outside observers, including the Pentagon:

> IO may be an attractive--but untested tool--in multiplying the effectiveness of Taiwan's military forces. As one of the world's largest producers of computer components, Taiwan has all of the basic capabilities needed to carry out offensive IO-related activities, particularly computer network attacks and the introduction of malicious code. As Taiwan increases its role in the manufacture of new computer warfighting systems, Taipei's capability to exploit its position for IO activities can be expected to increase substantially.[91]

These advantages are also recognized by information warfare advocates in the Taiwan military, who point to potential spin-on benefits of information technology development on the island:

> In the ROC, the accumulated information science and technology capability in the civilian sector (especially the computer virus attack and defense technology) is very outstanding. Therefore, the ROC military can utilize all the avenues to join forces with industry, government, academia, and research institutes to develop the key technology and assist defense organizations rapidly for establishing information warfare attack and defense capability.[92]

General Lin Chin-ching also highlights Taiwan's demographic advantages, arguing that "Taiwan's information warfare advantage, which cannot be matched by the mainland, is that all of our citizens have a very high level of universal education, with a solid communications infrastructure, and our related research on electronic anti-virus software and Internet defense products all being up to world-class level."

One area of proven Taiwanese IW capability, though not explicitly of military origin, is in the field of computer viruses. Among international virus experts, Taiwan is judged to be a leading laboratory for new strains. For example, a virus known as "Bloody" or "6/4," designed to protest the Tiananmen Square crackdown, was first discovered in Taiwan in 1990. In 1992, personnel from The Hague--with support from INTERPOL--investigated the dissemination of the "Michelangelo" virus by a Taiwan firm. In 1996, Taiwan virus writers developed and distributed a computer virus protesting Japanese claims to the Diaoyutai Islands. The following year, opponents of the Taiwan government developed a widely circulated Word-macro virus known as "Con-Air" which protested social problems on the island. The most virus of Taiwanese origin is the CIH virus, whose name is derived from the initials of its Taiwanese creator, Chen Ing-hau.[93] The CIH virus manipulates executable programs in Windows 95 and Windows 98, destroying floppy drives and hard disks.[94] The virus reportedly afflicted 360,000 Chinese computers on the

[91] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

[92] Lin Chin-ching, “Comparison of PRC, ROC Information Warfare Capabilities,” 1 March 2000, pp.68-73.

[93] “Computer Virus Author Revealed,” *Associated Press*, 30 April 1999.

[94] "Security Ministry of Checking Computer CIH Virus," *Xinhua*, 24 September 1998.

26th of April 1999, resulting in more than RMB1 billion in damages.[95] The date of the attack was the anniversary of the Chernobyl reactor disaster in Russia, leading some to re-label the virus as the "Chernobyl" virus. While Taiwan is known for creating viruses, it is also is well known for the efforts by researchers and corporations to combat computer viruses. Trend Micro--formerly known as Trend Micro Devices--is an industry leader in anti-virus software and, to a lesser extent, other network security products. Trend Micro was the first company to develop a response to the "Michelangelo" virus; it currently dominates the anti-virus software market in Japan. Trend Micro also has led in the area of virus recognition technology. Taiwan's Academia Sinica also has made impacts in the area of anti-virus software development.[96]

While Taiwan possesses considerable advantages in the IW area, it is also necessary to point out that Taiwan does suffer from some fiscal, bureaucratic and technical constraints. On a fiscal level, Taiwan's defense budgets have declined in recent years, in sharp contrast to the double-digit growth of the mainland's official defense expenditure. This financial pressure is exaserbated by procurement of large numbers of second generation fighter aircraft and other expected big-ticket items, such as ships, subs and theater missile defense systems. In order to support the costs of these purchases, as well as their maintenance expenses, advocates for IW complain that there is very little defense budget left for information warfare equipment.[97] The second constraint is bureaucratic opposition to IW. This factor is closely linked to the first, since the various service branches view interest in IW as coming at the expense of their conventional procurement programs. Third, Taiwanese IW officials complain of export restrictions on US key technology, which in turn impedes the development of high-technology equipment for information warfare.

Despite these obstacles, however, IW in Taiwan appears to be gaining ground, both in terms of strategy and operational capability. At a strategic level, the notion that information warfare will be the trump card in the Taiwan Strait defense operation in the future appears to be approaching military-wide consensus.[98] Even opponents concede that information warfare might provide Taiwan with more warning time of any irregular military activities and provide it with force multipliers to counterbalance the PRC’s electronic warfare against Taiwan. Moreover, the civilian leadership has become one of the most formidable proponents of IW in Taiwan. During the 2000 presidential election, Chen Shui-bian offered a defense concept known as “preemptive defense,” defined as maintaining strong deterrence posture during peacetime through the development of information warfare and long range precision strike capabilities. During wartime, however, Chen asserted that Taiwan should apply preemptive measures, including to information warfare, to suppress and destroy enemy’s C4I system and its warfighting and logistic capabilities.[99] With his victory over Lian Zhan and James Song in March 2000, it was widely expected that IW would assume higher priority within the Ministry of National Defense.

[95] Tim Neely and David Cowhig, "China: Information Security," U.S. Embassy (Beijing) report, June 1999. See also “Taiwan College Identifies Virus,” *Associated Press*, 29 April 1999; “CIH Virus Culprit Pegged?” *Wired News*, 29 April 1999; and Jeffrey Parker, “Taiwan Virus Suspect Free on Lack of Victims,” *Reuters*, 30 April 1999.

[96] Office of the Secretary of Defense, *The Security Situation in the Taiwan Strait*, Report to Congress Pursuant to the FY1999 Appropriations Bill, 26 February 1999.

[97] Lin Chin-ching, “Comparison of PRC, ROC Information Warfare Capabilities,” 1 March 2000, pp.68-73.

[98] Taipei Democratic Progress Party (DPP) Policy Committee, "White Paper on National Defense," 23 November 1999.

[99] Chen Sui-bian, *New Century, New Future: Chen Shui-bian’s Blueprint for the Nation – Volume 1: National Security* [xinshiji xinchulu: Chen Shui-bian guojia lantu – diyice: guojia anquan], (Taipei: Chen Shui-bian Presidential Campaign Headquarters, 1999), pp. 74-75.

Yet the ministry had already begun to organize the implementation of an information warfare capability even before Chen's election. In April 1999, advisory committee on information warfare strategic policy was created under the Ministry of National Defense, as well as an advisory body consisting of experts from the private sector. The existence of this information warfare research and training task force was revealed in May 1999 testimony by General Tang Fei to the Legislative Yuan.[100] Further discussion of this organization occured at a hearing on protection of Taiwan's computer systems from mainland Chinese intrusions, chaired by DPP legislators Lee Wen-chung and Tsai Ming-hsien. At the hearing, General Lin Chin-ching, director of CEIB offered his opinion that "we [Taiwan] are able to defend ourselves in an information war, but we will not initiate an offensive." The proposed committee was organized to invite experts and party representatives to study its comprehensive strategy to combat information warfare. To this end, the MND on 14 September 1999 launched the first of nine seminars "to beef up the military's ability regarding electronic warfare and to cope with the Chinese Communist threat."[101] The seminar was entitled the "2000 Telecommunications Information Security Lecture." It focused on communications security and computer virus protection, and aimed to "show the ministry's determination to ensure information security." The year 1999 also witnessed significant technical developments in the computer network defense area. According to the 2000 Defense White Paper, the ROC military deployed gateways, secure e-mail, and firewall systems, as well as a system of internal certification management and red teams.[102]

In late 1999, budget support for information warfare was a critical concern of the military leadership. In November, General Tang noted that should the Legislature approve an increased budget, priority would go toward adequate defenses against information warfare.[103] To bolster the case for IW, the Taiwan Ministry of National Defense laid down short-, intermediate-, and long-term targets.[104] The short-term target was focused on enhancing security of the information system and building a security mechanism. By integrating the various systems, the intermediate-term target was focused on developing capability to develop software and hardware for electronic warfare, improving frequency spectrum management, and enhancing electronic reconnaissance, electronic attack, electronic defense, and other electronic warfare capability. The long-term target was to continue to improve tactical and technological research and development, and to build an automated and digitized technological electromagnetic warfare. In addition, the military’s network and information systems were to be pushed underground with greater shielding, so as to protect them from damage caused by EMP blasts.

Chen Shui-bian's election as president heralded a new period in Taiwan's military IW program. Military leaders now highlight that the next five years will be the critical period in the PRC-ROC information warfare competition.[105] To achieve eventual dominance, General Lin Chin-ching of the CEIB in March 2000 outlined a seven-point plan:

[100] “Taiwan’s Information Warfare Task Force,” *Jane’s Defense Weekly*, 19 May 1999.
[101] "Taiwan Steps Up Training to Thwart PRC E-Warfare," *AFP*, 14 September 1999.
[102] 2000 White Paper.
[103] “Defense minister calls for budget increase,” *China Times*, 2 November 1999.
[104] “PRC, Taiwan Modern Warfare Viewed,” *Zhongyang ribao*, 22 November 1999.
[105] Lin Chin-ching, “Comparison of PRC, ROC Information Warfare Capabilities,” 1 March 2000, pp.68-73.

(1) Network Security

(a) Construct military communication security capability by improving overall monitoring and network node management.

(b) Implement overall directional electromagnetic protection.

(2) Establishment of Information Warfare Attack Action.

(a) Utilize civilian sector information science and technology capability to form an "information warfare experimental laboratory" that collects various types of computer viruses.

(b) Begin research and development on the key technologies of effective information weapons, including computer viruses, the electromagnetic impulse bombs, virus protection software, and network monitor control software.

(3) Joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Systems (C4ISR).

(a) Establish a C4ISR system combining each independent defense management information system.

(b) Implement measures to enhance the joint utilization of naval warfare intelligence, air defense information, and ground forces' operational systems.

(c) Integrate new types of radar and digital links.

(4) Transformation of Defense Management Information Systems

(a) Transform the existing system to meet core demands of the command, control, communications, computers, intelligence, surveillance, and reconnaissance system. In peacetime, support defense policy decisionmaking and strategic development. During wartime, support joint warfare command, and at the same time, through reorganization, improves the quality of information services, and provides transparency for the overall service across branches and systems in an information sharing environment.

(5) Construction of a High-Quality Communication and Information Environment.

(a) Implement network digitization, combining communication and information resources. Utilize wireless communication systems, aided by network management and virtual design to create a multimedia data environment.

(6) Public-Private Partnership

(a) Implement the out-sourcing of defense information construction, thereby expanding the armed forces' information capability.

(7) Critical Infrastructure Protection

(a) Create a national-level information warfare command organization, guided by the Executive Yuan, with the joint interior, foreign, defense, finance, education, legal, and economics departments and the national security bureau. The body would be focused on electric power, telecommunications, finance, transportation, and the nation's infrastructure security protection, with the goal of developing coordinated responses.

Progress in the implementation of this system could be seen in the August 2000 exercise known as "Hankuang #16," in which Red and Blue used computer viruses to attack each other's computer systems. the time of the exercise, the Taiwan military reportedly had gathered 2000 computer viruses.[106]

On 2 January 2001, the Taiwan military formally inaugurated its first information warfare (IW) force.[107] Minister of National Defense Wu Shih-wen had revealed the IW force plan to legislators on 22 November 2000 during the recess of a defense budget screening session held by the legislature's Defense Committee.[108] The unit, which is composed of almost one battalion of specialized troops, is independent of any service and is directly controlled by the office of the chief of the general staff. The command is in charge of researching and developing both defensive and offensive information warfare techniques, though the force was established mainly to cope with potential threats from China in the field, said Major General Chen Wen-chien, deputy director of the communication electronics and information bureau, under the defense ministry:

> We started planning for the new unit in 1998 as we saw the vast efforts made by the Chinese military to upgrade its information attack capabilities. It is to operate under the communication and information command of the Ministry of National Defense. The unit exists for two main purposes. The first is to maintain the security of computer networks in use in the armed forces. The second is to contribute to the overall information security of the country using its specialized knowledge of technology. The unit will become more consolidated after recruiting additional specialized personnel from different branches of the armed forces. For the moment, the unit is staffed by personnel with the Ministry of National Defense's recently-decommissioned `unified communication command,' the predecessor of the new Communications, Electronics, and Information Bureau. We did not widen our selection of personnel mainly because of restrictions brought by the ongoing Chingshih personnel streamlining project. But the current staff of the unit should be capable of handling their new tasks since what they are doing is almost the same as what they did before. Future personnel will be drawn from across all services.[109]

According to Chen, teams charged with maintaining network safety and pinpointing computer viruses within the military network will be set up in various regions across Taiwan in the future. While these countermeasures are primarily for defensive purposes, the head of this new command was clear about its potential for future offensive operations: “Should the People’s

[106] "Military to Test Computer Bugs," *AFP*, 8 August 2000.
[107] Fang Wen-hung, "Taiwan Information Warfare Command Established," *Taipei Central News Agency*, 02 January 2001.
[108] Brian Hsu, "Taiwan's First Information Warfare Group Enters Service," *Taipei Times*, 03 January 2001.
[109] Fang Wen-hung, "Taiwan Information Warfare Command Established," *Taipei Central News Agency*, 02 January 2001.

Liberation Army launch an informtion war against Taiwan, the military, armed with 1000 computer viruses, would be able to fight back."[110]

Conclusions

Driven by the threat from mainland China to its vulnerable information infrastructure, Taiwan has begun to implement a Revolution in Military Affairs, emphasizing modernization of technical systems, organization, and doctrine to meet new military challenges. Various RMA sectors, including electronic warfare, C4ISR, and information warfare, have received significant emphasis. Specialized units have been established, and comprehensive plans for integration of technology have been put forward. These efforts are bolstered by the island's advanced information technology sector, and the demographic benefits of an information-savvy population. Yet the RMA in the Taiwan military continues to suffer from important constraints, ranging from the usual atavistic opposition from status quo-oriented bureaucracies to the *sui generis* consequences of Taiwan's diplomatic isolation. Recent augmentation of the U.S.-Taiwan military relationship, in particular greater cooperation in the area of battle management and C4I, improve the possibility of overcoming these obstacles.

[110] Peter Harmsen, "Taiwan Has 1000 Computer Viruses to Fight Cyber War with China," *AFP*, 9 January 2000.